

|   |                          |   |
|---|--------------------------|---|
|  | <b>Comune di Trieste</b> | <b>Dipartimento Innovazione e Servizi al Cittadino</b><br><b>Servizio Trasformazione Digitale</b> |
|---|--------------------------|---|

***Verbale del gruppo di valutazione relativo alla procedura di affidamento diretto, mediante confronto di preventivi su MePA, per la realizzazione di un Security Assessment del Comune di Trieste e la redazione di un Piano di Sicurezza Informatica***

Il giorno 11/09/2024 alle ore 14:30, presso il Comune di Trieste, si è riunito il Gruppo di lavoro deputato alla valutazione delle offerte tecniche pervenute in relazione alla manifestazione d'interesse relativa alla realizzazione di un Security Assessment del Comune di Trieste e la redazione di un Piano di Sicurezza Informatica.

Il gruppo è costituito da:

- Giannina Ceschin – Dirigente del Servizio Trasformazione Digitale
- Massimo Spiller – P.O. Servizi IT e Digitalizzazione
- Carlo Gasprotich – supporto tecnico gruppo rete e security
- Mauro Rubieri – supporto tecnico al responsabile della transizione digitale

Sono pervenute in totale 13 proposte tecnico progettuali, corredate di relative offerte economiche, dalle imprese:

- AD CONSULTING
- AIZOON CONSULTING
- BOXXAPPS
- CROWE BOMPIANI
- DINOVA
- FASTWEB
- HWG SABABA
- MATICMIND
- MPG SYSTEM
- NAIS
- SECURE\_NETWORK
- SIELTE
- WIND TRE

Preso atto della documentazione pervenuta il gruppo di lavoro procede alla sua analisi e valutazione al fine di identificare l'offerente che meglio risponde alle esigenze dell'Ente in termini tecnici (affinità alle richieste, completezza delle risposte e dettaglio esplicativo personalizzato specificatamente per la realtà dell'Ente).

Le attività di valutazione del gruppo di lavoro sono proseguite nei giorni 12/09 alle ore 9.30, 16/09 alle ore 14:30, 18/09 alle ore 14:00 il giorno 23/09 alle ore 14:30 e il giorno 26/09 alle ore 9:30.

|   |                          |   |
|---|--------------------------|---|
|  | <b>Comune di Trieste</b> | <b>Dipartimento Innovazione e Servizi al Cittadino</b><br><b>Servizio Trasformazione Digitale</b> |
|---|--------------------------|---|

Come previsto nei documenti pubblicati, ai fini della scelta del contraente, sono stati valutati i seguenti elementi che costituiscono il fondamento delle ragioni della scelta:

- Tempistiche indicate nel cronoprogramma per lo svolgimento delle attività programmate (CRONO)
- Curriculum del personale (CV)
- Certificazioni inerenti alle tematiche di sicurezza (CERTIFICAZIONI)
- Possesso del "Cybersecurity Made in Europe Label" (MADE IN EUROPE)
- Documentate esperienze pregresse (ESPERIENZA)
- Proposta progettuale per l'analisi offline degli hash delle password degli utenti comunali (HASH)
- Proposta progettuale per la formazione e la campagna di phishing (PHISHING)
- Proposta progettuale di analisi delle vulnerabilità (VULNERABILITY)
- Proposta progettuale per il penetration test (PENETRATION)
- Contenuti del Piano di Sicurezza Informatica (PIANO SI)
- Supporto tecnico offerto per il periodo post-contrattuale (SUPPORTO EXTRA)

Dalla lettura della documentazione presentata da tutti gli offerenti, da un incrocio e sovrapposizione tra tutte le offerte presentate e da un'attenta analisi dei punti sopra elencati (anche e soprattutto in relazione alle peculiarità dell'Ente) è emerso che rispetto agli elementi di valutazione previsti in capitolato le imprese offerenti che si sono distinte e che hanno presentato offerte più affini alle necessità dell'Ente sono le seguenti:

- AIZOON CONSULTING
- FASTWEB
- HWG SABABA

Nello specifico:

- AIZOON CONSULTING è risultata eccellente negli aspetti relativi a "HASH", "PHISHING" e "PIANO SI", mentre è risultata buona nell'aspetto "CRONO" ed adeguata negli aspetti di "VULNERABILITY" e "PENETRATION"
- FASTWEB è risultata eccellente negli aspetti relativi a "HASH", "PHISHING", "PIANO SI" e "CRONO", mentre è risultata buona negli aspetti di "PENETRATION" e "VULNERABILITY"
- HWG SABABA è risultata eccellente negli aspetti relativi a "HASH", "PHISHING" e "PIANO SI", mentre è risultata buona negli aspetti di "PENETRATION", "VULNERABILITY" e "CRONO", inoltre, dispone della certificazione "MADE IN

|   |                          |   |
|---|--------------------------|---|
|  | <b>Comune di Trieste</b> | <b>Dipartimento Innovazione e Servizi al Cittadino</b><br><b>Servizio Trasformazione Digitale</b> |
|---|--------------------------|---|

EUROPE”

Per quanto riguarda le altre imprese offerenti, pur risultando tutte sufficienti in termini di adeguatezza formale alla risposta dei requisiti dell’indagine di mercato, dal confronto diretto tra quanto proposto dagli altri offerenti è emersa la seguente situazione:

- AD CONSULTING è risultata particolarmente carente nell’aspetto “VULNERABILITY” mancando di sufficiente dettaglio relativo all’implementazione specificatamente progettata per il Comune di Trieste, in particolare con gravi carenze relative all’analisi della rete esterna;
- BOXXAPPS è risultata particolarmente carente negli aspetti “HASH”, “PHISHING”, “VULNERABILITY” e “PENETRATION”, mancando di sufficiente dettaglio relativo alle implementazioni specificatamente progettate per il Comune di Trieste, in particolare sul coinvolgimento del reparto IT dell’Ente;
- CROWE BOMPIANI è risultata particolarmente carente negli aspetti “PHISHING”, “VULNERABILITY” e “PENETRATION”, mancando di sufficiente dettaglio relativo alle implementazioni specificatamente progettate per il Comune di Trieste, in particolare la parte “VULNERABILITY” prevede un alto impatto sul reparto IT dell’Ente oltre che apparire sottodimensionata rispetto alle esigenze dell’Ente;
- DINOVA è risultata particolarmente carente negli aspetti “HASH” e “PENETRATION” mancando di sufficiente dettaglio relativo alle implementazioni specificatamente progettate per il Comune di Trieste, in particolare sui criteri di analisi degli hash che verranno adottati nello specifico caso e sui passi operativi della procedura di penetration specificatamente calati nelle varie richieste dell’Ente;
- MATICMIND è risultata particolarmente carente negli aspetti “HASH”, “PHISHING”, “VULNERABILITY”, “PENETRATION” e “PIANO SI” mancando di sufficienti dettagli implementativi e, specificatamente su “HASH” e “PHISHING” le relazioni si limitano a descrivere premesse di partenza per progettare le attività;
- MPG SYSTEM è risultata particolarmente carente negli aspetti “PHISHING”, “VULNERABILITY” e “PENETRATION” mancando di sufficienti dettagli implementativi, inoltre si rileva una generale sgrammaticatura delle relazioni ed un bizzarro utilizzo dei tempi verbali, il che fa presupporre che tutte le relazioni (o parti di esse) siano state scritte da una qualche forma di intelligenza artificiale, ignorando del tutto le specifiche esigenze del Comune di Trieste;
- NAIS è risultata particolarmente carente nell’aspetto di “HASH”, dove presenta dettagli implementativi tecnici palesemente scadenti o non coerenti con la

|   |                          |   |
|---|--------------------------|---|
|  | <b>Comune di Trieste</b> | <b>Dipartimento Innovazione e Servizi al Cittadino</b><br><b>Servizio Trasformazione Digitale</b> |
|---|--------------------------|---|

realità del Comune di Trieste (dal punto di vista dell'hardware l'utilizzo di un laptop e dal punto di vista del software il dump diretto degli hash dal Domain Controller, presupponendo un ambiente Microsoft Active Directory di cui l'Ente è sprovvisto);

- SECURE\_NETWORK non è risultata particolarmente carente negli aspetti di confronto, ma non è apparsa sufficiente convincente nelle proposte relative al "PHISHING" (la formazione proposta è fumosa ed altamente impattante per l'Ente) e per quanto riguarda la "PENETRATION" traspare che è stata predisposta con un copia/incolla di altri documenti in quanto c'è una sezione totalmente fuori contesto (IPS/IDS e allow list di IP pubblici all'interno della parte relativa all'infrastruttura di rete LAN);
- SIELTE è risultata particolarmente carente negli aspetti "HASH", "PHISHING", "VULNERABILITY" e "PENETRATION" mancando di sufficienti dettagli implementativi e limitandosi a descrivere premesse metodologiche di progettazione, inoltre per quanto riguarda il "PIANO SI", non viene citato/descritto il "Piano di Risposta agli Incidenti Informatici";
- WIND TRE è risultata particolarmente carente negli aspetti "VULNERABILITY", "PENETRATION" e "PIANO SI" mancando di sufficienti dettagli implementativi e limitandosi a descrivere premesse metodologiche di progettazione (dal punto di vista hardware/infrastrutturale non è chiaro cosa è in carico all'offerente e cosa è in carico al reparto IT dell'Ente), inoltre per quanto riguarda il "PIANO SI", non viene citato/descritto il "Piano di Risposta agli Incidenti Informatici";

Al completamento della attività di valutazione sulle offerte tecniche si è proseguito con la valutazione delle offerte economiche delle imprese che hanno presentato le offerte più affini alle necessità dell'Ente.

Le offerte economiche valutate sono le seguenti:

Fastweb: 44.588,51 euro;

Aizoon: 39.900,00 euro;

Sababa: 39.500,00 euro;

Dall'analisi congiunta della parte tecnica e la parte economica il gruppo di lavoro propone per l'affidamento del servizio di 'Realizzazione di un Security Assessment del Comune di Trieste e la redazione di un Piano di Sicurezza Informatica' l'impresa HWG Sababa.

La seduta si è chiusa, redigendo il presente verbale, alle ore 13:00 del 26/09/2024.

|   |                          |   |
|---|--------------------------|---|
|  | <b>Comune di Trieste</b> | <b>Dipartimento Innovazione e Servizi al Cittadino</b><br><b>Servizio Trasformazione Digitale</b> |
|---|--------------------------|---|

Giannina Ceschin Giannina Ceschin

Massimo Spiller Massimo Spiller

Carlo Gasprotich Carlo Gasprotich

Mauro Rubieri Mauro Rubieri

**Signature:** *Giannina Ceschin*  
Giannina Ceschin (Oct 2, 2024 14:44 GMT+2)  
**Email:** giannina.ceschin@comune.trieste.it

**Signature:** *Massimo Spiller*  
Massimo Spiller (Oct 2, 2024 14:48 GMT+2)  
**Email:** massimo.spiller@comune.trieste.it

**Signature:** *Carlo Gasprotich*  
Carlo Gasprotich (Oct 2, 2024 14:42 GMT+2)  
**Email:** carlo.gasprotich@comune.trieste.it

**Signature:** *Mauro Rubieri*  
Mauro Rubieri (Oct 2, 2024 16:04 GMT+2)  
**Email:** mauro.rubieri@comune.trieste.it

# Verbale Valutazione Cybersecurity\_Finale

Final Audit Report

2024-10-02

|                 |   |
|-----------------|---|
| Created:        | 2024-10-02  |
| By:             | stefano cannizzaro (stefano.maria.cannizzaro@comune.trieste.it) |
| Status:         | Signed  |
| Transaction ID: | CBJCHBCAABAACMD7mUL_Pj_3cJuuW4JtniyCk_Ts5jzL                    |

## "Verbale Valutazione Cybersecurity\_Finale" History

-  Document created by stefano cannizzaro (stefano.maria.cannizzaro@comune.trieste.it)  
2024-10-02 - 12:42:02 PM GMT
-  Document emailed to Ginnina Ceschin (giannina.ceschin@comune.trieste.it) for signature  
2024-10-02 - 12:42:05 PM GMT
-  Document emailed to Massimo Spiller (massimo.spiller@comune.trieste.it) for signature  
2024-10-02 - 12:42:06 PM GMT
-  Document emailed to Carlo Gasprotich (carlo.gasprotich@comune.trieste.it) for signature  
2024-10-02 - 12:42:06 PM GMT
-  Document emailed to Mauro Rubieri (mauro.rubieri@comune.trieste.it) for signature  
2024-10-02 - 12:42:06 PM GMT
-  Email viewed by Carlo Gasprotich (carlo.gasprotich@comune.trieste.it)  
2024-10-02 - 12:42:33 PM GMT
-  Document e-signed by Carlo Gasprotich (carlo.gasprotich@comune.trieste.it)  
Signature Date: 2024-10-02 - 12:42:59 PM GMT - Time Source: server
-  Email viewed by Ginnina Ceschin (giannina.ceschin@comune.trieste.it)  
2024-10-02 - 12:43:57 PM GMT
-  Document e-signed by Ginnina Ceschin (giannina.ceschin@comune.trieste.it)  
Signature Date: 2024-10-02 - 12:44:25 PM GMT - Time Source: server
-  Email viewed by Massimo Spiller (massimo.spiller@comune.trieste.it)  
2024-10-02 - 12:45:35 PM GMT
-  Document e-signed by Massimo Spiller (massimo.spiller@comune.trieste.it)  
Signature Date: 2024-10-02 - 12:48:01 PM GMT - Time Source: server

 Email viewed by Mauro Rubieri (mauro.rubieri@comune.trieste.it)

2024-10-02 - 2:03:55 PM GMT

 Document e-signed by Mauro Rubieri (mauro.rubieri@comune.trieste.it)

Signature Date: 2024-10-02 - 2:04:32 PM GMT - Time Source: server

 Agreement completed.

2024-10-02 - 2:04:32 PM GMT